Program Research Project

SECURING CYBERSPACE: APPROACHES TO DEVELOPING AN EFFECTIVE CYBER-SECURITY STRATEGY

BY

LIEUTENANT COLONEL DOUGLAS S. SMITH
United States Army Reserve

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2011

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-05-2011	Program Research Project	

4. TITLE AND SUBTITLE

Securing Cyberspace: Approaches to Developing an Effective Cyber-Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
LTC Douglas S. Smith

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Col (Ret) Walt Wood
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Effective protection of cyberspace is a national security priority, essential to securing critical national assets. A comprehensive U.S. cyber-strategy is needed to deter, defend against, and respond to cyber-attacks. This paper examines the characteristics of hostile cyber-attacks and their implications to development of an effective strategy. U.S. cyber-strategy should incorporate concepts in three broad areas. First U.S. government and military policies should adopt a differentiated approach to security policy, centralize protection of military and government networks under U.S. Cyber Command using layered and dynamic defenses, and pursue a holistic interagency approach, as begun with the Comprehensive National Cyber-security Initiative. Second, the U.S. should exercise diplomatic means to seek international cooperation and collaboration on core areas of cyber-security. Third, the U.S. should develop a robust defense strategy tailored to deter likely potential adversaries and include mechanisms for managing escalation during a conflict in cyberspace.

15. SUBJECT TERMS

Cyber-attack, cyber-exploitation, cyber-crime, cyber-power, deterrence, U.S. Cyber Command, Internet

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC PROGRAM RESEARCH PROJECT

SECURING CYBERSPACE: APPROACHES TO DEVELOPING AN EFFECTIVE CYBER-SECURITY STRATEGY

by

Lieutenant Colonel Douglas S. Smith
United States Army Reserve

Topic Approved By
Colonel (Retired) Walt Wood

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Douglas S. Smith

TITLE: Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy

FORMAT: Program Research Project

DATE: 15 May 2011 WORD COUNT: 5,846 PAGES: 32

KEY TERMS: Cyber-attack, cyber-exploitation, cyber-crime, cyber-power, deterrence, U.S. Cyber Command, internet

CLASSIFICATION: Unclassified

Effective protection of cyberspace is a national security priority, essential to securing critical national assets. A comprehensive U.S. cyber-strategy is needed to deter, defend against, and respond to cyber-attacks. This paper examines the characteristics of hostile cyber-attacks and their implications to development of an effective strategy. U.S. cyber-strategy should incorporate concepts in three broad areas. First U.S. government and military policies should adopt a differentiated approach to security policy, centralize protection of military and government networks under U.S. Cyber Command using layered and dynamic defenses, and pursue a holistic interagency approach, as begun with the Comprehensive National Cybersecurity Initiative. Second, the U.S. should exercise diplomatic means to seek international cooperation and collaboration on core areas of cyber-security. Third, the U.S. should develop a robust defense strategy tailored to deter likely potential adversaries and include mechanisms for managing escalation during a conflict in cyberspace.

SECURING CYBERSPACE: APPROACHES TO DEVELOPING AN EFFECTIVE CYBER-SECURITY STRATEGY

Cyberspace has become part of the fabric of the modern world. Internet usage is growing exponentially, from one million internet users in 1992, to 1.2 billion users in 2007, to over two billion in 2010.[1] Society increasingly relies on cyberspace tools to regulate infrastructure critical to daily life, such as electric power grids, global finance, banking, transportation, healthcare, and telecommunications. The nation's military depends on networks for command and control, communications, intelligence, logistics and weapons systems. Although few would deny the benefits that cyberspace has brought to nearly every facet of life, reliance on free access to cyberspace makes society vulnerable to disruptions caused by malicious attackers, cyber-criminals or even teenage hackers.

Protecting cyberspace is a national security priority. President Obama's National Security Strategy (NSS) acknowledges that threats to cyber-security "represent one of the most serious national security, public safety, and economic challenges we face as a nation."[2] The Quadrennial Defense Review (QDR) Report states that in the 21st century, "modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."[3] These statements support the assertion that the U.S. has a vital national interest in cyberspace, with free and unencumbered access for innovation, global commerce and communications, and with robust security to protect the digital infrastructure that powers critical national functions. The NSS articulates the strategic objective that supports this interest: "deter, prevent, detect, defend against, and quickly

recover from cyber intrusions and attacks."[4] A comprehensive cyber-strategy is needed to achieve this objective (ends) that includes conceptual approaches (ways) in three broad areas: (1) U.S. government and military policies for cyberspace defense, (2) international influence in cyberspace, and (3) deterrence of cyber-attacks.

The Nature of Conflict in Cyberspace

Development of a comprehensive cyber-security strategy requires an understanding of cyberspace and the nature of conflict within it. This section discusses definitions for cyberspace, cyber-power, cyber-attack and cyber-exploitation and recent examples of how cyber-conflict has embroiled the physical world.

Since the term was coined in 1984[5], *cyberspace* has been described in numerous contexts within science fiction, academia, government, and the military. Many sources describe cyberspace as a global operational domain and compare its qualities to the physical domains: land, sea, air and space. Human utilization of each domain followed from technological innovation. The space domain, for example, was unimportant to society before development of rockets and satellites. Today's communications would be impossible without operational capabilities in space. Advances in electronics and computers created cyberspace, the first man-made domain, and opened it to human exploration and exploitation.

The Joint Chiefs of Staff define cyberspace as a global domain within the information environment, encompassing the "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] The domain is framed by "the use of electronics and the electromagnetic spectrum to create, store, modify,

exchange and exploit information."[7] The implication of this definition is that cyberspace represents not just the technical aspects of the medium, such as networks and computers, but also the information itself and the human element that shapes and interprets the information.

Protecting strategic interests in cyberspace requires effective application of cyber-power. Daniel Kuehl, Director of the Information Strategies Concentration Program at the National War College, defines cyber-power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[8] This definition is reminiscent of Mahan's concept of sea-power: "a nation's ability to enforce its will upon the sea."[9] The nation wielding sea-power has capabilities to guarantee free access across the oceans for its own purposes and interests and to prevent adversaries from impeding the same. Similarly, the nation wielding cyber-power has capabilities to patrol cyberspace and take actions to secure its own interests within cyberspace and prevent adversaries from impeding the same. Unlike the physical domains, however, cyberspace creates effects in all five domains. Consequently, cyber-power is applicable to all operational domains and all elements of national power.

Conflict in cyberspace can occur in one of two forms: cyber-attack or cyber-exploitation. Although there is no consensus of what constitutes a cyber-attack, all are comprised of a deliberate action taken to "alter, disrupt, deceive, degrade, or destroy" systems or networks in cyberspace.[10] The scale of attacks can vary widely, ranging from the inconvenience of being locked out of a network to complete shutdown of critical control systems.

Cyber-attacks share four important characteristics.[11] First, the indirect effects of the attack are often more consequential than the direct effects. An attack against the controls of a power grid, for example, could cause blackouts, similar to what might occur during natural disasters. The indirect effects might outweigh the direct effects, such as interruptions to commerce, creation of opportunities for crime, public outcry and reduced investment. For example, cyber-attacks to the power grid caused several wide-spread blackouts in Brazil and Paraguay in 2005, 2007, and 2009. Although the most recent outage only lasted for two hours, the incident created the perception that the infrastructure in South America is vulnerable. International perceptions disproportionately bruised Brazil's reputation, undermining confidence in their ability to safely host the 2016 Olympic Games and soccer's 2014 World Cup.[12]

Second, the technology to launch a cyber-attack is relatively inexpensive and readily available. As a result, non-state actors have adopted cyber-attacks as a weapon of choice. Small groups can develop sophisticated capabilities to conduct cyber-attacks against large, well resourced entities for economic or political purposes. For example, a three-week cyber-war raged in Estonia in 2007. The dispute erupted when Russians protested the Government of Estonia's announcement that it would remove a Soviet war memorial, the "Bronze Soldier of Tallinn."[13] Russian hackers attacked numerous government agencies, banks, and news organizations, intermittently shutting down networks and disrupting life in Estonia.[14] The attacks appeared to be perpetrated by Russian individuals inside and outside of Russia, without proven support from the Russian Federation. The conflict illustrates what cyber-war may look like in the future:

small, technically advanced groups attack the digital infrastructure of nations in pursuit of a political objective.

Third, cyber-attacks may be highly asymmetric. A common weapon in cyberspace is the *botnet*, a large number of infected computers remotely controlled by a master computer. A botnet grows when a virus infects ordinary computers across the internet, creating virtual links between them without users' knowledge. The perpetrator can remotely activate his army of computers against specific targets, to overwhelm networks, block or disrupt access to systems, or infect other computers and networks.[15] One example is the Mariposa botnet, made up of 13 million infected computers, created and controlled by just a few individuals.[16] After infecting an unsuspecting computer, the program monitored activity for passwords and banking and credit card information. The internet's openness allows a single user to amplify his influence.

Fourth, perpetrators can conceal their identities with relative ease if they seek anonymity. For example, the Conficker Worm is a propagating and mutating virus that has infected an estimated 10 million computers, creating the framework for a powerful botnet ready to launch an attack at its creator's signal. Despite unprecedented international collaboration and even a bounty offer standing since 2009, the identity and motives of the worm's creators remain a mystery. A botnet this large could theoretically "paralyze the infrastructure of a major Western nation."[17]

Cyber-exploitation involves the use of offensive actions within cyberspace but unlike cyber-attacks normally does not seek to disrupt the normal functioning of the targeted network or systems. The objective of cyber-exploitation is usually to obtain information for illegitimate purposes, including espionage, theft of confidential

information such as credit card or personal information, or other criminal reasons.[18] For example, China has directed cyber-espionage efforts against the U.S. Department of Defense since 2002, with successful theft of 10 to 20 terabytes of data from military networks.[19]

As the world becomes more interconnected, cyber-power increasingly is "exerting itself as a key lever in the development and execution of national policy."[20] An effective cyber strategy will benefit numerous national efforts, including counter-terrorism, economic development, fighting crime, diplomatic engagement, and intelligence gathering.

U.S. Government and Military Policies for Cyberspace Defense

Governance of cyberspace is an elusive concept. The term *governance* is misleading because governments currently exercise little control over internet policy or protocols. Instead, an evolving collection of private and commercial organizations determine policies and protocols by consensus to keep the internet functioning smoothly. One such organization is the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non-profit corporation responsible for assigning domain names, the unique identifier that gives information a place to exist on the internet ("www.microsoft.com," for example, is the assigned domain name for the Microsoft Corporation). ICANN has a government advisory committee open to any national government, but members may only advise ICANN's Board of Directors and do not have voting rights on board policies.[21] Other forums are responsible for other cyberspace functions, such as communications standards and core internet functions.[22] These organizations have evolved in an ad hoc manner driven mainly by the need to resolve technical issues. But where once technical problem-solving was an academic

notion necessary for establishing cyber infrastructure, today the need to fight cyber-exploitation and cyber-attack lends a heightened urgency for proper conduct within cyberspace. Given the present state of governance, public policy-makers should seek to develop greater influence on certain aspects of cyberspace, rather than adopt true governance.[23] Government initiatives should include three approaches to cyber-security: (1) a differentiated approach to security policy, (2) a centralized approach to protect military cyber-assets under U.S. Cyber Command, and (3) a holistic interagency approach, as begun with the Comprehensive National Cybersecurity Initiative.

First, the U.S. government should develop a differentiated approach to cyber-security, with the intent of prioritizing the wide variety of cyber-attacks and cyber-exploitations and appropriately focusing counter-measures. The first step is to prioritize cyber-attacks and cyber-exploitations with regard to their possible consequences. On one end of the spectrum are the nuisance hackers who probe networks thousands of times each day. On the other end is the sophisticated cyber-attack that causes damages commensurate with an act of war. This approach should classify cyber capabilities as *indispensable*, *key* or *other*. *Indispensable* cyber would include critical military capabilities or civil security capabilities that the country could not be without even for a short time.[24] *Key* cyber also include critical infrastructure but for which temporary workarounds are possible. This may include electric grids, financial networks, transportation systems, and certain military or intelligence capabilities whose exploitation would damage national security. The vast bulk of cyber capabilities remaining would fall into the *other* category. Next, security measures should be tailored for each category. For *indispensable* cyber, the federal government should provide

security directly. Activities should include actively monitoring for attacks, providing cyber defenses and redundant systems. For *key* cyber, the federal government should develop policies and regulations that require minimum levels of protection for cyber capabilities that reside with private or state control and provide adequate resources for law enforcement and security cooperation with entities that have responsibility for key cyber capabilities. For *other* cyber, the government could encourage improved cyber-security through education, incentives, or voluntary participation in government security programs.

Second, U.S. Cyber Command (CYBERCOM) has assumed responsibility for protection of critical government and military cyber assets. It achieved full operational capability on November 3, 2010, as a four-star, sub-unified command under U.S. Strategic Command.[25] CYBERCOM's three-prong mission is to: (1) operate and defend DoD networks, (2) prepare to conduct full-spectrum military cyberspace operations, and (3) defend U.S. freedom of action in cyberspace.[26] CYBERCOM executes its first mission with a layered defense of the Global Information Grid (GIG). The outer most layer of protection is "ordinary hygiene," which includes keeping malware protection, firewall, and anti-virus software up to date on 15,000 networks within the .mil domain and seven million computers.[27] Diligent hygiene blocks about half of attempted intrusions. The next line of defense is "perimeter security," which monitors traffic in and out of DoD networks.[28] CYBERCOM has limited the number of access ports to DoD systems from the internet, creating cyber choke points where it can more effectively marshal defenses. Perimeter security blocks an additional 30-40% of attempted intrusions. Finally, CYBERCOM conducts dynamic defenses to block the last 10% of

attempted intrusions. Dynamic defense systems act in real-time as "part sensor, part sentry, part sharpshooter."[29] They continuously monitor traffic, automatically identify intruders and block access. In contrast, static defenses, such as hygiene activities, wait and react to intruders after they have penetrated the network. The National Security Agency (NSA) leads the initiative to develop dynamic defenses. In addition to technical capabilities, NSA will incorporate foreign intelligence to anticipate threats. Effective unity of effort is possible with U.S. Army General Keith Alexander acting as both CYBERCOM's Commander and NSA's Director. A challenge remaining for CYBERCOM will be to develop mechanisms to extend cyber protection to key cyber capabilities that reside outside of DoD-controlled networks. Although General Alexander cites the importance of the principle, he admits that older cyber-systems powering electric grids, banking and transportation systems are inherently more difficult to defend.[30] The military also depends on commercial and unclassified networks for much of its communications and records-keeping. Lessons learned from CYBERCOM's efforts to protect the GIG should be applied to cyber-security for critical civilian sectors.

Third, the U.S. should pursue a holistic interagency approach to cyber-security. The Comprehensive National Cybersecurity Initiative (CNCI) is an excellent template for success. The initiative was launched by the Bush administration in January, 2008, in response to a series of cyber-attacks on multiple federal agency networks. It was intended to unify agencies' approach to cyber-security. Under the Obama administration, it has evolved into a broader cyber-security strategy. The CNCI defines 12 initiatives to facilitate collaboration among federal and state governments and the private sector that ensure an organized and unified response to cyber attacks.[31] For

example, the Trusted Internet Connections program, an initiative led by the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), consolidates access ports to Federal Government systems, much as CYBERCOM has done for military systems.[32] Fewer access ports are more easily monitored and defended. Another initiative involves deployment of an intrusion detection and prevention system for civilian government networks. Developed by DHS, the EINSTEIN 2 program was deployed to automatically detect unauthorized or malicious network traffic across U.S. Government networks and send real-time alerts to the U.S. Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cyber Security Division within DHS charged with coordinating the federal response to cyber-attacks.[33] DHS is also working to pilot technology developed by the NSA as EINSTEIN 3, to conduct "real-time full packet inspection and threat-based decision-making" with the ability to automatically respond to cyber threats before harm is done.[34] Another initiative calls for connecting strategic cyber operations centers to enhance situational awareness across agency networks and systems and foster interagency collaboration and coordination. The intent is for the National Cybersecurity Center (NCSC) within the DHS to connect six existing cyber centers within DHS, DoD, FBI, NSA, and Office of Director of National Intelligence (ODNI) to share information with each other through relationships and liaison officers.[35] Together, the centers create common situational awareness among key cyber functions, including cyber-intelligence, counter-intelligence, cyber-crime investigation and law enforcement, civil and defense collaboration, and intrusion detection and response.

These initiatives show remarkable progress on creating a holistic, interagency approach to protecting government systems against cyber-attack. Like other interagency efforts, however, the CNCI will be challenged by competing agency interests, control of significant resources targeted for cyber-security, and by public debate about the proper role for federal regulations. In 2009, for example, the Director of the NCSC resigned in protest of the increasingly prominent role played by the NSA in cyber efforts. He argued in favor of checks and balances by separating security powers among government agencies, and cited "threats to democratic processes … if all top-level government network security and monitoring are handled by any one organization."[36] This initiative continues amid public debate on the appropriate role that government oversight and control should play in balancing protection against cyber-attack with free and open access to cyberspace.[37]

International Influence in Cyberspace

Private sector entities and individuals have few effective and legal alternatives to respond to a cyber-attack or cyber-exploitation. The first line of defense is to strengthen their passive defensive measures, including dropping services that are targeted or closing firewall ports to deny access to key systems. These measures cannot completely protect systems against increasingly sophisticated attackers and deny the victim the benefits of key services or connections.[38] The second option is to report the cyber-attack or cyber-exploitation to the authorities for prosecution. Questions of global jurisdiction, however, complicate prompt investigation and prosecution. If a U.S. company is cyber-attacked in its Japanese offices by the Russian mob through a server located in Brazil, where does the jurisdictional authority lie for prosecuting the attack?[39] To improve effectiveness of cyber efforts in a globally connected world, the U.S. should

exercise diplomatic means to seek common ground among countries and intergovernmental organizations for fighting against cyber-attacks and cyber-exploitation and to influence international partners to collaborate on core areas of cyber-security.

Effective policy-making to encourage international cooperation requires an understanding of how different cultures give rise to different attitudes and norms about fighting cyber-attacks. The U.S., for example, prefers to engage international law enforcement to investigate and catch cyber criminals.[40] International cooperation could resolve jurisdictional issues when perpetrators conduct cyber-attacks across state lines. INTERPOL conducts a similar function for fighting international crime by providing liaison between law enforcement authorities among its 188 member countries.[41] It provides a model for international cooperation that could apply to cyber-crime, as well.

In contrast, Russia argues that the U.S. approach would lead to interference in its internal affairs. Russia jealously protects non-interference, an "immutable principle of international law," as a pillar of her sovereignty.[42] Russia tends to be wary of American motives, which it claims have political and ideological goals aimed at undermining Russian independence and its sphere of influence in Eastern Europe. Russia's actions and policies also conveniently protect its own population of patriotic hackers, an educated and empowered volunteer militia within cyberspace. These were the foot-soldiers during the cyber-conflict that occurred during the Georgia-Russia conflict of 2008.[43] One day after Russia invaded Georgia, the StopGeorgia.ru forum began conducting a series of denial-of-service attacks against Georgian government websites that disabled several key websites during the invasion. The StopGeorgia.ru forum was run by sophisticated hackers who published lists of vetted targets that patriotic Russian

hackers attacked. Although the Russian Government distanced itself from the hacker activity, it clearly enjoyed the benefits and tacitly supported the community. International law enforcement cooperation, as espoused by the U.S., could target these non-state hackers.

China has a third view. Chinese authorities closely monitor Chinese networks and take aggressive steps to filter or block what the government considers "politically troublesome content," such as references to democracy, civil liberties, Chinese political dissidents, and other concepts contrary to Red ideology.[44] The alleged intent of China's internet crack-down is to protect civil order. Supporters of free speech decry these practices as censorship and a pretext for the government to tighten its control over daily life and solidify its power. The three approaches illustrate the divergent attitudes toward cyberspace and underscore the complexity in attempting to influence international norms and behavior.

With an understanding of cultural differences about cyberspace, American diplomatic efforts should seek common ground among countries to cooperate in promoting cyber-security and combating cyber-attacks. The U.S. should advocate that cyberspace is a global commons whose usefulness is contingent upon its security. Diplomatic pressure is needed to influence countries to adopt collaborative practices in finding and blocking cyber attacks. One such collective approach is the Council of Europe's Convention on Cybercrime. Thirty countries have ratified the convention, including the U.S., and 17 others are signatories. The convention requires that signatories enact stringent laws against cyber-crime and take steps to investigate and prosecute violators. The convention also directs participating countries to cooperate

with one another in such matters as reciprocal law, extradition, and mutual assistance.[45] A weakness of the convention is that while it mandates public action, it establishes few means to verify compliance. The convention is currently open for signatures, but differences in cultural attitudes discussed above present barriers to wider acceptance. The U.S. should use diplomatic pressure to encourage wider acceptance of the Convention's principles.

The concept of a sanctuary state should be developed to bring international pressure to bear on states who fail to discharge their duty to prevent cyber-attacks. The 9/11 attacks on the World Trade Centers and the Pentagon introduced a new paradigm for fighting terrorism. The resulting doctrine prescribed that the U.S. would not only fight terrorists but also the regimes that harbored and sheltered them. Similarly, a state that fails to prosecute cyber-criminals, or who gives safe haven to individuals or groups that conduct cyber-attacks against another country, may be defined as a sanctuary state.[46] Policy-makers should seek to develop a common understanding of cyber-sanctuary states within the international community and intergovernmental organizations. Diplomatic pressure or other actions could then be taken to coerce the sanctuary state to exercise its duty to prevent cyber-attacks against entities in other countries.

Deterrence of Cyber-attacks

The National Security Strategy states that one strategic objective is to prevent cyber-attacks.[47] But strategic documents and cyberspace initiatives focus on detecting and intercepting cyber-attacks, with scant attention on developing methods to deter cyber-attacks. Common arguments against the effectiveness of cyber-deterrence include the difficulties in accurately attributing the source of cyber-attacks, the murky legal status of cyber-attacks as an act of war, and the lack of proportionate response

options that carry sufficient weight to deter a cyber-attack. Given the serious potential consequences of a successful attack against critical infrastructure, the U.S. should develop a robust defense strategy tailored to deter likely potential adversaries, include mechanisms for managing escalation during a cyber crisis, and give due consideration to complexities such as the presence of “patriotic hackers.”

The central concept for deterring an adversary from taking action against the U.S. is to influence the adversary’s decision-making calculus, with the result that he perceives inaction as preferable to action. The U.S. Joint Operating Concept describes three core concepts for deterrence: (1) pose a credible threat to impose costs to the adversary if he takes the undesired action, (2) deny the benefits to the adversary of the undesired action, and (3) encourage restraint by offering consequences for inaction.[48] In the context of cyberspace, determining specific techniques to impose cost or deny benefits is complicated by the wide array of potential adversaries, which range from hackers set on breaking into sensitive systems for the sheer technical challenge, terrorist use of cyber-attack as an asymmetric weapon, to nation-state use of cyber-espionage or cyber-attack to support kinetic operations. The individual hacker’s motivations and perception of risk are radically different from those of a nation-state. Effective approaches to deterrence, therefore, must be tailored based on a sophisticated understanding of the adversary’s “unique and distinct identities, values, perceptions, and decision-making processes.”[49]

In developing tailored deterrence strategies, policy-makers must first identify who is being deterred. A common perception holds that the difficulty of attribution (identifying potential or actual cyber-attackers) arrests any meaningful attempt to develop cyber-

deterrence. The relative ease of concealing one's identity within cyberspace does introduce uncertainty in attributing attacks in real-time. But deterrence planning should be done within a larger geo-political context. Following the differentiated approach principle, deterrence should focus on potential high-end cyber-attacks. Low-end cyber-attacks, such as hackers defacing websites, may be adequately deterred with on-going efforts to improve defenses. The high-end attacks most in need of deterrence, however, are likely to be conducted within the context of a political or ideological agenda. Terrorist groups, rogue states, and near-peer states such as China and Russia will continue to develop cyber-power in the future. They will likely use cyber-exploitation and cyber-attacks as part of an overall strategy directed toward achieving political objectives.[50] Knowledge of potential adversaries and their motives and methods does not require real-time attribution during a crisis. Tailored deterrence strategies should be developed in peacetime for actors with known grievances against the U.S. What America must avoid is facing a cyber-attacker whose identity is known but for whom an effective and proportionate response has not already been conceived and critically reviewed. A cyber-attacker would hope to catch the U.S. unprepared. A strong, declared policy, tailored to each important adversary, would begin the process of developing viable deterrence.

Should a non-state actor wish to remain anonymous, the difficulty of accurate attribution of the attack is a limitation to deterrence actions during a crisis. A non-state actor could launch a cyber-attack from within a covering state without its knowledge, complicating efforts to identify the attacker. A criminal group might use a botnet, for example, to launch coordinated attacks from hundreds or thousands of computers

located in multiple non-hostile countries.[51] A retaliatory response in cyberspace might damage networks in non-hostile countries or unrelated systems. If the perpetrator launched the attack from within a sanctuary state, the victim would likely have difficulty discriminating the degree of the state's involvement. One scenario is an attack launched with full approval of the sanctuary state authorities and carried out with state assets. Another possibility is an attack that is tacitly encouraged by the state but carried out with non-state assets. Responses would vary according to the degree of state involvement. Intelligence and diplomatic resources should be brought to bear to complement technical attribution. In under-developed states with little cyberspace integrated into society, an appropriate cyber-response may not be available, reducing the range of options for policy-makers to economic, diplomatic or military responses.

The threat of retaliation (imposing costs) is the cornerstone of classical deterrence theory. Before considering options for retaliation, policy-makers must determine the legal status of a cyber-attack. CYBERCOM's commander affirmed that the "international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace."[52] A full legal analysis of how the Law of War applies to cyber-attack is outside the scope of this paper. But deterrence planning must include a decision-making structure at the national level to assess cyber-attacks, determine their legal status as acts of war, and formulate a range of possible responses within the bounds of proportionality.

Deterrence by imposing costs or denying intended benefits to the attacker should consider all elements of national power, as well as actions purely in cyberspace, to calibrate a deterrent posture. Technical efforts to improve cyber defenses, by denying

access to networks or deploying dynamic defenses to stop intrusions, may alter the adversary's cost-benefit analysis sufficiently to dissuade some cyber-attacks, particularly less sophisticated adversaries with fewer cyber resources. When an adversary fails to penetrate a targeted system and cannot deliver the expected results, he must decide whether to accept additional risk by escalating the attack. Deterrence plans should deny benefits by developing ways to degrade the effectiveness of messages. As a "creative and cultural commons," cyberspace is increasingly becoming the "predominant domain of political victory or defeat."[53] An extremist cyber-attacker, for example, may judge his attack's effectiveness by how widely his ideological message spreads, captures publicity and lends some degree of credibility to his cause. Indirect effects could continue on blogs and forums long after the direct effects of a compromised system have been eliminated. A deterrence strategy should consider non-technical ways to neutralize the message, such as information operations and counter-messages. For significant cyber-attacks, policy-makers should consider using other forms of national power, such as diplomatic and economic pressure. These may deter states who have the potential to employ cyber-weapons, or who might shield groups within their borders from launching cyber-attacks. These tools could also be used to offer incentives for adversaries to refrain from cyber-attacks.

As with classical deterrence, cyber-deterrence planning should specify methods to manage escalation during a crisis, including transparency and signaling of intentions. A nation could in principle respond to a cyber-attack with a kinetic counter-attack, as a way to inflict unacceptable costs on a hostile opponent. Classical deterrence seeks to calibrate a response proportionate to the damage inflicted by an attack. For cyber-

deterrence, the difficulty in discriminating indirect effects from direct effects and in linking physical damages with a digital attack clouds the ability to determine a measured and proportionate response. A kinetic response might therefore be viewed as overly provocative and could result in undesired escalation of hostilities.[54] In conventional situations, adherence to international norms of behavior benefits stability, such as pre-announcing large troop movements, maritime "rules of the road,"[55] diplomatic engagement, and treaties and agreements that prescribe accepted behavior among nations. In contrast, legitimate cyber-activities are completely intermingled with illegitimate cyber-activities. A cyber-attack may be difficult to distinguish from a cyber-exploitation or hacker. Military use of cyberspace may be indistinguishable from civilian use. A culture of secrecy pervades American cyber policies and compromises the ability to signal national intentions. The U.S. should pursue policies to make its cyber intentions and capabilities more transparent, while protecting its technical know-how. To start, a strong policy of deterrence against cyber-attacks should be declared and promulgated in the National Security Strategy.

Managing escalation during a conflict would be facilitated by a workable framework for cyber early warning. Ned Moran, Professor at Georgetown University, proposed a useful five-stage model for helping to anticipate cyber-attacks.[56] Stage 1 is recognition and assessment of latent tensions. Both state and non-state actors manifest background tensions long before actual attacks. These should be assessed within a global geo-political context and with regard to capability to conduct cyber as well as physical operations. Stage 2 is cyber reconnaissance. Prior to initiating hostilities in cyberspace, adversaries are likely to probe one another, to discover vulnerabilities and

strengths, just as adversaries would do on a conventional battlefield.[57] Stage 3 is the initiating event. In the 2007 Estonian cyber-war, the initiating event was the removal of the Soviet memorial in Tallinn. It caused tensions to boil over in the form of riots in Moscow as well as in cyberspace.[58] Stage 4 is cyber mobilization. Following the initiating event, adversaries organize groups in cyberspace, recruit sympathetic supporters, and vet targets. For example, Chinese hackers mobilize support for political causes on message boards and chat rooms. In 2008, Chinese users created an anti-CNN forum to refute "the lies and distortion of facts from the Western Media."[59] Keen observation of internet forums and blogs combined with foreign intelligence gathering could identify when cyber soldiers are mobilizing and proactively raise the cyber alert status. Stage 5 is the cyber-attack itself. The effectiveness of the attack depends on the sophistication of the perpetrators and the degree of reconnaissance and preparation performed. The U.S. should carefully observe the cyber activity of actors with known grievances against America, to look for signs of one of the five stages of the early warning model. Responses taken earlier in the process will more likely prevent escalation of the conflict to a more serious stage.

The presence of patriotic hackers will complicate efforts for deterrence and managing escalation during a conflict. As hostilities build, both sides of a conflict are likely to experience a surge of patriotic hackers, who act independently or in grass-roots groups to harass the opposing side. These activities are outside of government control but may be difficult to distinguish from a state-sponsored cyber-attack.[60] The cyber-war during the Russian invasion of Georgia in 2008 is an instructive example. The StopGeorgia.ru project was originated by a grassroots network of Russian hackers

inside and outside the Russian Federation. Russia denied official involvement and direct support of the project, but it clearly benefited from the cyber-attacks during the invasion and did nothing to stop them.[61] A more worrisome scenario could occur with a phenomenon known as “catalytic cyber-conflict.” This refers to a conflict where a third party instigates conflict between two countries by launching a cyber-attack disguised to resemble one country attacking the other.[62] This occurred in July 2009 when a number of U.S. and South Korean government websites shut down over the Independence Day weekend. Suspicion immediately fell on North Korea, and one U.S. congressman even called for a military counter-attack. The likely perpetrator was not North Korea, however, but a hacker community in another country.[63] The incident underscores the fragility of stability in cyberspace and the need for the U.S. to focus on major cyber threats from adversaries with known grievances against the U.S.

The Way Ahead

Protecting access to cyberspace serves American vital interests. A comprehensive cyber-security strategy, developed now while the U.S. is in a preeminent position in this newly evolving domain, will best utilize resources to solidify American cyber-power.

Government and military policies are needed to improve cyber-security of critical networks and systems. Key conclusions and recommendations include:

- The U.S. should adopt a policy of differentiation among cyber-attacks to prioritize response planning towards attacks that target more critical national assets.

- CYBERCOM and NSA's defense-in-depth of military and government systems illustrate an effective template for static and active cyber defenses.
- Best practices for cyber-security learned from CYBERCOM should be applied more broadly to critical civilian sectors.
- Initiatives under the CNCI show significant progress on creating a holistic, interagency approach to protecting government systems.

As cyberspace grows exponentially, the world becomes more interconnected and prone to shared vulnerabilities within cyberspace. The U.S. needs to exert international influence to encourage cooperation and collaboration in order to improve cyber-security.

- Cultural differences about cyberspace present barriers to international cooperation, norms and responsible behavior within cyberspace.
- The U.S. should use diplomatic means to encourage wider acceptance of the principles promulgated in the Convention on Cybercrime.
- The international community should develop the concept of the cyber sanctuary state and pressure states who fail to prevent cyber-attacks that emanate from within their borders.

Policy-makers should develop plans not just for improving cyber defenses but preventing cyber-attacks by implementing plans that include tailored deterrence against known adversaries with cyber-capabilities and tools to manage escalation during a cyber-crisis.

- Deterrence planning need not wait for accurate attribution real-time during a crisis, but rather should be developed within a broader geo-political context with regard to adversaries with known grievances against the U.S.

- Attribution of non-state actors who wish to remain anonymous will be difficult. The state from which the non-state actor launches his attack may be complicit with the perpetrator, tacitly allow the attack, or be completely unaware of the attack.
- The presence of patriotic hackers complicates deterrence planning and crisis escalation management.

More complete development of these approaches to a cyber-strategy require study of the resources (means) to support the conceptual concepts (ways) discussed in this paper and to assess the degree of risk arising from identified gaps.

The importance of cyberspace to national security is growing commensurately with increasing band-width, faster computing power, and greater reliance on digital networks to power critical parts of modern society. The U.S. cyber-strategy must evolve, too, to keep pace with innovative competitors in order to maintain freedom of cyberspace.

Endnotes

[1] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 51-52.

[2] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May, 2010), 27.

[3] Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February, 2010), 37.

[4] Obama, *National Security Strategy,* 27.

[5] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 24. Dr. Kuehl cites the William Gibson science fiction novel, *Neuromancer*.

[6] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010, amended through January 31, 2011), 92.

[7] Kuehl, "From Cyberspace to Cyberpower," 28. A similar definition is found in U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, September 17, 2006, incorporating Change 2, March 22, 2010), II-22.

[8] Ibid., 38.

[9] William Oliver Stevens and Allan Westcott, *A History of Sea* Power (New York: Doubleday, 1920), 443, quoted in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 38.

[10] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), 10-11.

[11] Ibid., 80-81.

[12] CBS News / Associated Press, "Lights Back On In Brazil After Blackout," November 11, 2009, http://www.cbsnews.com/stories/2009/11/10/world/main5607148.shtml?tag=mncol;lst;1 (accessed February 27, 2011).

[13] Jeffrey Carr, *Inside Cyber* Warfare (Sebastopol, CA: O'Reilly Media, 2010), 3.

[14] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 475-476.

[15] Clay Wilson, "Cyber Crime," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 420.

[16] U.S. Congress, House of Representatives, Committee on Armed Services, *U.S. Cyber Command: Organizing for Cyberspace Operations*, 111th Congress, hearing held September 23, 2010 (Washington, DC: U.S. Government Printing Office, 2010), 37.

[17] Carr, *Inside Cyber Warfare,* 12-13.

[18] Ibid., 11.

[19] Ibid., 4.

[20] Kuehl, "From Cyberspace to Cyberpower," 39.

[21] Harold Kwalwasser, “Internet Governance,” in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 498.

[22] Starr, “Toward a Preliminary Theory of Cyberpower,” 67.

[23] Ibid., 67.

[24] Franklin D. Kramer, “Cyberpower and National Security: Policy Recommendations for a Strategic Framework,” in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 7.

[25] U.S. Air Force, “Cyber Command Achieves Full Operational Capability,” release number 031110, November 3, 2010, http://www.afspc.af.mil/pressreleasearchive/story.asp?id=123229293 (accessed April 21, 2011).

[26] U.S. Strategic Command, “Factsheet: U.S. Cyber Command,” http://www.stratcom.mil/factsheets/Cyber_Command (accessed April 18, 2011).

[27] William J. Lynn, III, “Remarks at Stratcom Cyber Symposium,” May 26, 2010, http://www.defense.gov/Speeches/Speech.aspx?Speechid=1477 (accessed April 18, 2011).

[28] Ibid.

[29] Cheryl Pellerin, “Lynn: Cyberspace is the New Domain of Warfare,” (Washington, DC: American Forces Press Services, October 18, 2010), http://www.defense.gov/news/newsarticle.aspx?ID=61310 (accessed November 20, 2010).

[30] U.S. Congress, *U.S. Cyber Command*, 40.

[31] National Security Council, *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed April 18, 2011).

[32] Lynn, “Remarks at Stratcom Cyber Symposium.”

[33] Ibid.

[34] Department of Homeland Security, “Privacy Impact Assessment for the Initiative Three Exercise,” March 18, 2010, (Washington DC: Department of Homeland Security, 2010): 3.

[35] The White House, “National Cybersecurity Center Policy Capture,” http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf (accessed April 21, 2011).

[36] Shaun Waterman, “U.S. Cybersecurity Head Quits, Citing Growing Role of Spy Agencies,” (Washington DC: UPI, March 11, 2009), http://www.upi.com/Top_News/Special/2009/03/11/US-cybersecurity-head-quits-citing-growing-role-of-spy-agencies/UPI-64411236692969/ (accessed April 21, 2011).

[37] Director Beckstrom argued that improved checks and balances would result by keeping the operational agencies separate, a policy contrary to the principle of unity of effort. Though he could have, he did not advocate for legislative or judicial oversight, similar to Congressional oversight of the military or of the intelligence community. Legislative or Judicial oversight would provide effective checks and balances while maintaining the benefits of interagency collaboration and cooperation.

[38] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* 67.

[39] Ibid.

[40] Carr, *Inside Cyber Warfare,* 34-35.

[41] International Criminal Police Organization, "About INTERPOL," http://www.interpol.int/public/icpo/default.asp (accessed April 25, 2011).

[42] Carr, *Inside Cyber Warfare,* 35.

[43] Ibid., 15-17.

[44] Kwalwasser, "Internet Governance," 517.

[45] Council of Europe, *Convention on Cybercrime*, European Treaty Series No. 185 (Budapest: November 23, 2001).

[46] Carr, *Inside Cyber Warfare,* 67.

[47] Obama, *National Security Strategy,* 27.

[48] U.S. Joint Chiefs of Staff, *Deterrence Operations Joint Operations Concept* (Washginton, DC: U.S. Joint Chiefs of Staff, December 2006), 20.

[49] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 303.

[50] Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security,* ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 314.

[51] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 141.

[52] U.S. Congress, *U.S. Cyber Command*, 40.

[53] Kramer, "Cyberpower and National Security," 19.

[54] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 309.

[55] Ibid., 312.

[56] Carr, *Inside Cyber Warfare,* 179-182.

[57] Ibid., 181.

[58] Ibid., 182.

[59] Ibid.

[60] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 310.

[61] Carr, *Inside Cyber Warfare,* 15-17.

[62] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* 312.

[63] Carr, *Inside Cyber Warfare,* 79-83.